PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : G11B 20/00, H04H 1/00

A1

(11) International Publication Number: WO 00/00969

(43) International Publication Date: 6 January 2000 (06.01.00)

(21) International Application Number: PCT/US99/13482

(22) International Filing Date: 16 June 1999 (16.06.99)

(30) Priority Data:
09/106,213 29 June 1998 (29.06.98) US

(71) Applicant: ARIS TECHNOLOGIES, INC. [US/US]; 1972 Massachusetts Avenue, Cambridge, MA 02140 (US).

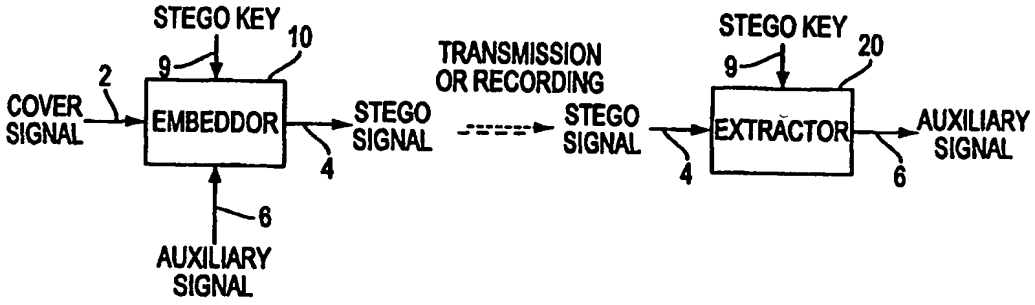
(72) Inventor: PETROVIC, Rade; 2 Castle Drive, Wilmington, MA 01887 (US).

(74) Agents: DELUCA, Vincent, M. et al.; Rothwell, Figg, Ernst & Kurz, Suite 701 East, Columbia Square, 555 13th Street N.W., Washington, DC 20004 (US).

(81) Designated States: CA, CN, IN, JP, KR, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: APPARATUS AND METHOD FOR EMBEDDING AND EXTRACTING INFORMATION IN ANALOG SIGNALS USING REPLICA MODULATION



(57) Abstract

Apparatus and methods are provided for embedding or encoding auxiliary signals (6) into an analog host or cover signal (2). A replica of the cover signal or a portion of the cover signal in a particular domain (time, frequency or space) is generated according to a stego key (9) specifying modification values to specified parameters of the cover signal. The replica signal is then modified by an auxiliary signal corresponding to the information to be embedded, and inserted back into the cover signal. Embedded auxiliary signals are extracted by generating replicas of received signals and correlating the replicas with the received signals.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania
AM	Armenia
AT	Austria
AU	Australia
AZ	Azerbaijan
BA	Bosnia and Herzegovina
BB	Barbados
BE	Belgium
BF	Burkina Faso
BG	Bulgaria
BJ	Benin
BR	Brazil
BY	Belarus
CA	Canada
CF	Central African Republic
CG	Congo
CH	Switzerland
CI	Côte d'Ivoire
CM	Cameroon
CN	China
CU	Cuba
CZ	Czech Republic
DE	Germany
DK	Denmark
EE	Estonia
ES	Spain
FI	Finland
FR	France
GA	Gabon
GB	United Kingdom
GE	Georgia
GH	Ghana
GN	Guinea
GR	Greece
HU	Hungary
IE	Ireland
IL	Israel
IS	Iceland
IT	Italy
JP	Japan
KE	Kenya
KG	Kyrgyzstan
KP	Democratic People's Republic of Korea
KR	Republic of Korea
KZ	Kazakstan
LC	Saint Lucia
LI	Liechtenstein
LK	Sri Lanka
LR	Liberia
LS	Lesotho
LT	Lithuania
LU	Luxembourg
LV	Latvia
MC	Monaco
MD	Republic of Moldova
MG	Madagascar
MK	The former Yugoslav Republic of Macedonia
ML	Mali
MN	Mongolia
MR	Mauritania
MW	Malawi
MX	Mexico
NE	Niger
NL	Netherlands
NO	Norway
NZ	New Zealand
PL	Poland
PT	Portugal
RO	Romania
RU	Russian Federation
SD	Sudan
SE	Sweden
SG	Singapore
SI	Slovenia
SK	Slovakia
SN	Senegal
SZ	Swaziland
TD	Chad
TG	Togo
TJ	Tajikistan
TM	Turkmenistan
TR	Turkey
TT	Trinidad and Tobago
UA	Ukraine
UG	Uganda
US	United States of America
UZ	Uzbekistan
VN	Viet Nam
YU	Yugoslavia
ZW	Zimbabwe

APPARATUS AND METHOD FOR EMBEDDING AND EXTRACTING INFORMATION IN ANALOG SIGNALS USING REPLICA MODULATION

BACKGROUND OF THE INVENTION

Field of the Invention

This invention relates to apparatus and methods for encoding or embedding and decoding or extracting information in analog signals, such as audio, video and data signals, either transmitted by radio wave transmission or wired transmission, or stored in a recording medium such as optical or magnetic disks, magnetic tape, or solid state memory.

Background and Description of Related Art

The present invention is concerned with techniques for embedding and extracting auxiliary information within an existing signal, such as an audio or video signal.

An area of particular interest to certain embodiments of the present invention relates to the market for musical recordings. Currently, a large number of people listen to musical recordings on radio or television. They often hear a recording which they like enough to purchase, but don't know the name of the song, the artist performing it, or the record, tape, or CD album of which it is part. As a result, the number of recordings which people purchase is less than it otherwise would be if there was a simple way for people to identify which of the recordings that they hear on the radio or TV they wish to purchase.

Another area of interest to certain embodiments of the invention is copy control (also referred to as digital watermarking). There is currently a large market for audio software products, such as musical recordings. One of the problems in this market is the ease of copying such products without paying those who produce them. This problem is becoming particularly troublesome with the advent of recording techniques, such as digital audio tape (DAT), which make it possible for copies to be of very high quality. Thus it would be desirable to develop a scheme which would prevent the unauthorized copying of audio recordings, including the unauthorized copying of audio works broadcast over the airwaves. It is also desirable for copyright enforcement to be able to insert into program material such as audio or video signals digital copyright information identifying the copyright holder, which information may be detected by appropriate apparatus to identify the copyright owner of the program, while remaining imperceptible to the listener or viewer.

Yet another field of interest relating to the present invention pertains to automatic royalty tracking and proof of performance of copyrighted material or commercial advertisements, by which copyright owners are able to track public performances or broadcasts of their material for royalty payment purposes, and advertisers are able to confirm that commercials which they have paid for were actually broadcast at the proper time and date.

Still another area of interest to the present invention relates to integrity verification or tampering detection, wherein the creator of an audio or audiovisual work can determine whether it has been altered, modified or incorporated into another work.

Various prior art methods of encoding additional information onto a source signal are known. For example, it is known to pulse-width modulate a signal to provide a common or encoded signal carrying at least two information portions or other useful portions. In U.S. Patent No. 4,497,060 to Yang (1985) binary data is transmitted as a signal having two differing pulse-widths to represent logical "0" and "1" (e.g., the pulse-width durations for a "1" are twice the duration for a "0"). This correspondence also enables the determination of a clocking signal.

With respect to systems in which audio signals produce audio transmissions, U.S. Patent Nos. 4,876,617 to Best et al. (1989) and 5,113,437 to Best et al. (1992) disclose encoders for forming relatively thin and shallow (e.g., 150 Hz wide and 50 dB deep) notches in mid-range frequencies of an audio signal. The earlier of these patents discloses paired notch filters centered about the 2883 Hz and 3417 Hz frequencies; the later patent discloses notch filters but with randomly varying frequency pairs to discourage erasure or inhibit filtering of the information added to the notches. The encoders then add digital information in the form of signals in the lower frequency indicating a "0" and in the higher frequency a "1". In the later Best et al. patent an encoder samples the audio signal, delays the signal while calculating the signal level, and determines during the delay whether or not to add the data signal and, if so, at what signal level. The later Best et al. patent also notes that the "pseudo-random manner" in moving the notches makes the data signals more difficult to detect audibly.

Other prior art techniques employ the psychoacoustic model of the human perception characteristic to insert modulated or unmodulated tones into a host signal such that they will be masked by existing signal components and thus not perceived. See, e.g. Preuss et al., U.S. Patent No. 5,319,735, and Jensen et al., U.S. Patent No. 5,450,490. Such techniques are very expensive and complicated to implement, while suffering from a lack of robustness in the face of signal distortions imposed by perception-based compression schemes designed to eliminate masked signal components.

The prior art fails to provide a method and an apparatus for embedding and extracting auxiliary analog or digital information signals onto analog audio or video frequency signals for producing humanly perceived transmissions (i.e., sounds or images) such that the audio or video frequency signals produce substantially identical humanly perceived transmission prior to as well as after encoding with the auxiliary signals (in other words, the embedded information is transparent to the listener or viewer), which is also robust to a high degree of signal distortions caused by noisy transmission mediums, etc. The prior art also fails to provide relatively simple and inexpensive apparatus and methods for embedding and extracting signals defining auxiliary information into audio or video frequency signals for producing humanly perceived audio transmissions.

SUMMARY OF THE INVENTION

The present invention provides apparatus and methods for embedding or encoding, and extracting or decoding, auxiliary (analog or digital) information in an analog host or cover signal in a way which has minimal impact on

the perception of the source information when the analog signal is applied to an appropriate output device, such as a speaker, a display monitor, or other electrical/electronic device.

The present invention further provides apparatus and methods for embedding and extracting machine readable signals in an analog cover signal which control the ability of a device to copy the cover signal.

In summary, the present invention provides for the encoding or embedding of an auxiliary signal in an analog host or cover signal, by generating a replica signal from the cover signal, modifying the replica signal as a function of the auxiliary signal, and inserting the modified replica signal back into the analog cover signal to provide a stego signal. The invention further provides for the extraction of embedded auxiliary signals from stego signals by generating a replica of the stego signal, and correlating the replica with the stego signal.

According to another aspect of the invention, apparatus for embedding and extracting auxiliary signals in an analog cover signal, is provided, comprising a replica generator for generating a replica signal from the cover signal, a modulator for modifying the replica signal as a function of the auxiliary signal, an adder for inserting the modified replica signal back into the analog cover signal to produce a stego signal, a receiver for receiving the stego signal, a generator for generating a replica signal from the stego signal, a modulator for modifying the received stego signal as a function of the replica signal of the received stego signal, and an extractor for extracting the auxiliary signal by filtering the modified received stego signal.

The term cover signal as used hereinafter refers to a host or source signal, such as an audio, video or other information signal, which carries or is intended to carry embedded or hidden auxiliary data.

BRIEF DESCRIPTION OF THE DRAWINGS

These and other aspects of the present invention will become more fully understood from the following detailed description of the preferred embodiments in conjunction with the accompanying drawings, in which:

FIG. 1 is a block diagram of a data signal embedding and extracting process utilized by the present invention;

FIG. 2 is a block diagram of one embodiment of the embeddor 10 of Fig. 1;

FIG. 3 is a block diagram of one embodiment of the embedded signal generator 11 of Fig. 2;

FIG. 4 is a block diagram of one embodiment of the data signal extractor 20 according to the present invention;

FIG. 5 is a block diagram of one embodiment of a replica generator which produces a cover signal replica shifted in frequency from the original; and

FIGs. 6(a)-6(c) are graphs showing a set of orthogonal functions used in the creation of an amplitude-shifted replica according to one embodiment of the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is directed to a method and apparatus for embedding information or data onto a cover signal, such as an audio signal, video signal, or other analog signal (hereinafter called a "cover signal"), by generating a replica of the cover signal within a

predefined frequency, time and/or space domain, modulating the replica with an auxiliary signal representing the information to be added to the cover signal, and then inserting the modulated replica back into the cover signal. The invention can implemented in a number of different ways, either by software programming of a digital processor, in the form of analog, digital, or mixed-signal integrated circuits, as a discrete component electronic device, or a combination of such implementations. The replica is similar to the cover signal in time and frequency domain content, but different in certain parameters as specified by a stego key, which is not generally known, but which is known at authorized receiving apparatus.

Referring to Fig. 1, the invention employs an embeddor 10 to generate a stego signal 4, which is substantially the same in terms of the content and quality of information carried by a cover signal 2. For instance, where cover signal 2 is a video or audio signal, the stego signal 4 will produce essentially the same video or audio program or information when applied to an output device such as a video display or loudspeaker.

A stego key 9 is used to determine and specify the particular region of the time, frequency and/or space domain of the replica where the auxiliary signal 6 is to be embedded, as well as the parameters of the embedding process.

The embeddor then appropriately modulates or modifies the replica and adds the replica back into the cover signal to obtain a stego signal 4. Stego signal 4 can be transmitted, or stored in a storage medium such as magnetic tape, CD-ROM, solid state memory, and the like for later recall and/or transmission. The embedded

auxiliary signal is recovered by an extractor 20, having knowledge of or access to the stego key 9, which operates on the stego signal 4 to extract the auxiliary signal 6. The embedding process can be expressed by the formula:

$$\bar{s}(t) = s(t) + \sum_i w_i(t) \qquad (1)$$

where $\bar{s}(t)$ represents the stego signal 4, $s(t)$ represents the cover signal 2, and $w_i(t)$ is the i-th hidden signal 8 (see Fig. 2), also known as a watermark. In this regard, the embeddor can be used to insert multiple auxiliary signals 6 simultaneously, using a different stego key 9 for each signal. In the case where only a single auxiliary signal 6 is to be inserted, a single stego key 9 is used, and there would be only one hidden signal $w(t)$. In equation (1) and hereinafter, a one-dimensional signal (i.e. a signal varying according to a single dimension, such as time) is considered for purposes of simplicity in explanation; however, the present invention is not limited to one-dimensional signals but can be readily extended to multidimensional signals such as images (two dimensions), video (three dimensions), etc., by defining t as a vector.

According to the present invention, a replica of the cover signal 2 itself is used as a carrier for the auxiliary signal 6. Because the replica is inherently similar to the cover signal in terms of frequency content, no analysis of the cover signal is necessary in order to hide an auxiliary signal, such as a digital watermark.

In contrast, according to the prior art techniques discussed above, auxiliary signals are embedded in the form of a pseudorandom sequence (Preuss et al.) or in the form of multiple tones distributed over the frequency band of the cover signal (Jensen et al.). In order to "hide"

such signals so that they are perceptively transparent, it was necessary to perform an analysis of the cover signal in the frequency domain to make the watermark signal imperceptible to the observer. Such analysis is based on the phenomenon that human perception will not detect a smaller signal in the presence of a larger signal if the two signals are sufficiently similar. This phenomenon is usually known as the masking effect.

The embedded signal 8 according to the present invention can be expressed by the formula:

$$w_i(t) = g_i m_i(t) r_i(t) \qquad (2)$$

where $g_i < 1$ is a gain (scaling factor) parameter determined by tradeoff considerations of robustness versus transparency, $m_i(t)$ is the auxiliary signal 6, wherein $|m_i(t)| \leq 1$, and $r_i(t)$ is a replica of the cover signal 2. The gain factor g_i can be a predetermined constant for a given application, or it can be adaptable, such that dynamic changes in transparency and robustness conditions can be taken into account. For example, in highly tonal musical passages the gains can be lower, while for spectrally rich or noisy audio signals the gains can be higher, with equivalent levels of transparency. In an alternate embodiment, the embeddor can perform an extractor process simulation to identify signals having less than desirable detectability, and increase the gain accordingly.

Fig. 2 shows a block diagram of one preferred embodiment of the embeddor 10. As shown, the cover signal 2, stego key 9, and auxiliary signal 6 are inputted to an embedded signal generator 11. The embedded signal generator generates replica $r_i(t)$ from cover signal 2

according to the stego key 9, modulates or modifies the replica $r_i(t)$ with auxiliary signal 6 ($m_i(t)$), scales the result using gain parameter g_i, and generates an embedded signal 8 ($w_i(t)$). The embedded signal 8 is then added to the cover signal 2 ($s(t)$) in an adder 12, to produce the stego signal 4 ($\bar{s}(t)$).

The replica $r_i(t)$ is obtained by taking a portion of the cover signal 2 within a specified time, frequency and/or spatial domain as specified by the stego key 9, and then making slight modifications to the signal portion, also as specified by the stego key 9. The modifications to the signal portion need to be small to ensure that the replica remains similar to the cover signal as judged by the human psychoacoustic-psychovisual systems, but such modifications must be large enough to be detectable by an appropriately designed extractor having knowledge of or access to the stego key 9. As will be discussed below, a number of different types of modifications have been found to satisfy these requirements.

Equation (2) reveals that the replica $r_i(t)$ is modulated by the auxiliary signal $m_i(t)$ according to a process known as product modulation. Product modulation results in a broadening of the spectrum of the embedded signal proportionally to the spectral width of the auxiliary signal. In order to make the spectrum of the embedded signal similar to the spectrum of the cover signal (to preserve the transparency of the embedding process) the spectrum of the auxiliary signal must be narrow in comparison with the lowest frequency in the spectrum of the replica. This requirement imposes a limit on the capacity of the auxiliary channel, and dictates that low frequency components of the cover signal are unsuitable for inclusion in the creation of the replica.

In a preferred embodiment of the invention, the modulating signal (auxiliary signal) m(t) is a binary data signal defined by the formula:

$$m(t)=\sum_{n=1}^{N} b_n h(t-nT) \qquad (3)$$

where N is the number of binary digits or bits in the message, $b_n \epsilon (-1,1)$ is the n-th bit value, T is the bit interval, and h(t) represents the shape of the pulse representing the bit. Typically, h(t) is obtained by low-pass filtering a rectangular pulse so as to restrict the spectral width of the modulating (auxiliary) signal.

Fig. 3 illustrates the details of an embedded signal generator 11 used to generate a single embedded data message. The cover signal 2 is filtered and/or masked in filtering/masking block 30 to produce a filtered/masked signal 31. The filter/mask block 30 separates regions of the cover signal used for different embedded messages. For example, the filter/mask block may separate the frequency band region 1000-3000 Hz from the cover signal in the frequency domain, may separate the time interval region t=10 seconds to t=30 seconds from the cover signal in the time domain, or may separate the upper right spatial quadrant region of the cover signal in the spatial domain (such as where the cover signal is an MPEG, JPEG or equivalent signal) which separated region would then be used for auxiliary signal embedding.

The filtered/masked signal 31 is comprised of the selected regions of the cover signal, as specified by stego key 9, which are then used for creation of the replica signal 41. The signal 31 is then inputted to a replica creator 40, where predetermined parameters of the signal are modified, as specified by stego key 9, to

create the replica $r_i(t)$ 41. The replica 41 is then modulated by the auxiliary signal $m_i(t)$ in multiplier 42a, and the resultant signal is then scaled in multiplier 42b according to the selected gain factor g_i to produce embedded signal component 8 (i.e., $w_i(t)$ in equation (2)). The embedded signal component 8 is then added back to the cover signal 2 in adder 12 (Fig. 2) to obtain the stego signal 4. In order to maintain synchronization between the cover signal 2 and the embedded signal component 8, inherent processing delays present in the filter/mask block 30 and replica creator block 40 are compensated for by adding equivalent an delay in the cover signal circuit path (between the cover signal input and the adder 12) shown in Fig. 2.

It is further possible to embed multiple auxiliary data signals in the cover signal 2, by using multiple embedded signal generators, each using a different stego key to modify a different feature of the cover signal and/or to use different regions of the cover signal, so as to produce multiple embedded signal components each of which are added to the cover signal 2. Alternatively, the different data signals may be embedded in a cascade fashion, with the output of one embeddor becoming the input of another embeddor using a different stego key. In either alternative interference between embedded signal components must be minimized. This can be accomplished by using non-overlapping frequency, time or space regions of the signal, or by selecting appropriate replica creation parameters, as disclosed below.

A block diagram of an extractor used to recover the auxiliary data embedded in the stego signal is shown in Fig. 4. The stego signal 4 is filtered/masked in filter/mask module 30a to isolate the regions where the

auxiliary data is embedded. The filtered signal 31a is inputted to replica creator 40a where a replica $\bar{r}_i(t)$ 41a of the stego signal is generated in the same manner as the replica $r_i(t)$ of the cover signal in the replica creator block 40 in the embeddor, using the same stego key 9. The replica $\bar{r}_i(t)$ of the stego signal 4 can be expressed by the formula:

$$\bar{r}_i(t) = r_i(t) + \sum_i g_i R(m_i(t) r_i(t)) \approx r_i(t) \quad (4)$$

where $R(m_i(t) r_i(t))$ represents the replica of the modulated cover signal replica. For sufficiently small gain factors g_i the replica of the stego signal is substantially the same as the replica of the cover signal.

In the extractor 20, the replica $\bar{r}_i(t)$ 41a is multiplied by the stego signal 31a in multiplier 42c to obtain the correlation product:

$$c(t) = \bar{r}_i(t)\bar{s}(t) \approx r_j(t)s(t) + \sum g_i m_i(t) r_i(t) r_j(t) \quad (5)$$

In designing the replica signal, one objective is to obtain spectra of the products $r_j(t)s(t)$ and $r_i(t)r_j(t)$, $i \neq j$, with little low frequency content. On the other hand, the spectra of the product $r_j(t)r_j(t) = r_j^2(t)$ contains a strong DC component, and thus the correlation product $c(t)$ contains a term of the form $g_i m_i(t) \text{mean}(r_j^2)$, i.e., $c(t)$ contains the scaled auxiliary signal $m_i(t)$ as a summation term.

In order to extract the auxiliary signal $m_i(t)$ from the correlation product $c(t)$, filtering is performed on

c(t) by filter 44, which has a filter characteristic matching the spectrum of the auxiliary signal. For example, in the case of a binary data signal with a rectangular pulse shape, the matched filtering corresponds to integration over the bit interval. In the case of digital signaling, the filtering operation is followed by symbol regeneration in a regenerator 46. A multiplicity of the extracted data symbols is then subjected to well-known error detection, error correction, and synchronization techniques to verify the existence of an actual message and proper interpretation of the content of the message.

One preferred embodiment of a replica creator 40 is shown in Fig. 5. In this embodiment, a replica signal 41 is obtained by shifting the frequency of the filtered cover signal 31 by a predetermined offset frequency f_i as specified by the stego key 9. This shifting process is also known as single sideband amplitude modulation, or frequency translation. In addition to the processing shown in Fig. 5, a number of different techniques known in the art are available to perform this process.

Blocks 52 and 54 represent respective phase shifts of the input signal s(t). To achieve the desired frequency shift, the relationship between the phase shifts must be defined as:

$$\varphi_1(f) - \varphi_2(f) = 90° \qquad (6)$$

The respective phase-shifted signals are multiplied by sinusoidal signals with frequency f_i in respective multipliers 56a and 56b. Block 58 denotes a 90° phase shift of the sinusoidal signal applied to multiplier 56b. The resulting signals are then combined in summer 59.

Thus, the replica signal 41 can be expressed as:

$$r_i(t)=s(t,\varphi_1)\sin(2\pi f_i t)\pm s(t,\varphi_2)\cos(2\pi f_i t) \quad (7)$$

where $s(t,\varphi_i)$ denotes signal s(t) phase-shifted by φ_i. The sign - or + in the summation process represents a respective shift up or down by f_i. According to psychoacoustic models published in the literature, better masking may be achieved when the shift is upward. Accordingly, in the preferred embodiment subtraction is used in equation (7). In a special case $\varphi_1=90°$ and $\varphi_2=0°$, such that equation(7) becomes:

$$r_i(t)=s_h(t)\sin(2\pi f_i t)\pm s(t)\cos(2\pi f_i t) \quad (8)$$

where $s_h(t)$ is a Hilbert transform of the input signal, defined by:

$$s_h(t)=1/\pi \int_{-\infty}^{\infty} \frac{s(x)}{t-x}dx \quad (9)$$

The Hilbert transform may be performed in software by various known algorithms, with equation (8) being suitable for digital signal processing. For analog signal processing, it is easier to design a circuit pair that maintains the 90° relative phase shifts throughout the signal spectrum, than to perform a Hilbert transform.

The particular frequency offset f_i can be chosen from a wide range of frequencies, and specified by the stego key. Multiple auxiliary signals can be inserted into the same time, frequency and/or space domain of the same cover signal, by having a different frequency offset value, to thus achieve a "layering" of auxiliary signals and increase auxiliary channel throughput.

The frequency offset also may be varied in time

according to a predefined secret pattern (known as "frequency hopping"), to improve the security of a digital watermark represented by the auxiliary information.

The particular choice of frequency offset values is dependent upon the conditions and parameters of the particular application, and can be further fine tuned by trial and error. According to experimental results, optimal signal robustness in the presence of channel distortion was achieved where the frequency offset value was larger than the majority of spectrum frequencies of the modulating auxiliary signal $m(t)$. On the other hand, optimal transparency was achieved where the frequency offset value was substantially smaller than the lowest frequency of the cover signal. As an example, for audio signal embedding a cover signal above 500 Hz was used with a frequency offset of 50 Hz, while the modulating signal was a binary data signal with a bit rate of 25 bps.

In an alternative embodiment of a replica creator, the replica is generated by shifting the phase of the filtered/masked portion 31 of the cover signal by a predetermined amount defined by a function $\varphi_i(f)$ for an i-th embedded signal. In this case, the replica generators 40 and 40a are linear systems having a transfer function defined as:

$$H_i(f) = A_i e^{j\varphi_i(f)} \qquad (10)$$

Where A_i is a constant with respect to frequency, j is the imaginary number $\sqrt{-1}$, and $\varphi_i(f)$ is the phase characteristic of the system. Circuits described by equation (10) are known in the art as all-pass filters or

phase correctors, and their design is well-known to those skilled in the art.

This embodiment is particularly suitable for auxiliary signal embedding in audio signals, since the human audio sensory system is substantially insensitive to phase shifts. The functions $\varphi_i(f)$ are defined to meet the objective that the product of the replica and the cover signal contain minimal low frequency content. This can be achieved by maintaining at least a 90° shift for all frequency components in the filtered/masked signal 31. Multiple embedded messages have been implemented with little interference where the phase shift between frequency components of different messages is larger than 90° for the majority of the spectral components. The exact choice of the function $\varphi_i(f)$ is otherwise governed by considerations of tradeoff between cost and security. In other words, the function should be complex enough so that it is difficult for unauthorized persons to determine the signal structure by analyzing the stego signal, even with the known cover signal, yet it should be computationally inexpensive to implement. A function hopping pattern which switches between different functions at predetermined intervals as part of the stego key can be used to further enhance security.

A special class of phase shift functions, defined by

$$\varphi_i(f) = \tau_i f \tag{11}$$

where τ_i is a constant, results in time shift replicas of the cover signal. This class of functions has special properties in terms of cost/security tradeoff, which are

beyond the scope of the present disclosure and will not be further treated here.

According to a further alternate embodiment of the invention, the replica generator obtains the replica signal by amplitude modulation of the cover signal. The amplitude modulation can be expressed by the equation

$$r_i(t)=a_i(t)s(t) \tag{12}$$

where $a_i(t)$ is a class of orthogonal functions. Figs. 6(a)-6(c) illustrate a set of three elementary functions $a_1(t)$, $a_2(t)$, and $a_3(t)$ used to generate amplitude shifted replica signals, with each function being defined over the interval (0,T) where T equals the bit interval of the auxiliary signal. Longer replicas are generated by using a string of elementary functions. Post-correlation filtering in the extractor is performed by integration over the interval T, and the auxiliary channel bit $b_{j,n}$ is extracted according to the formula $\overline{b}_{j,n}=\text{sign}(A_{j,n})$, where:

$$A_{j,n}=\int_{(n-1)T}^{nT} c(t)\,dt \approx \int_{(n-1)T}^{nT} a_j(t)s^2(t)\,dt+\sum_i g_i\int_{(n-1)T}^{nT} m_i(t)s^2(t)a_i(t)a_j(t)\,dt$$
$$\approx g_i\int_{(n-1)T}^{nT} m_j(t)s^2(t)\,dt \tag{13}$$

The above approximations hold, since

$$\int_0^T a_j(t)\,dt=0, \quad \int_0^T a_i(t)a_j(t)\,dt=0, \text{ for } i\neq j, \text{ and } a_j^2(t)=1$$

As is apparent from equation (13), the sign of $A_{j,n}$ (and the received bit value) depends on the sign of $m_j(t)$ during the n-th bit interval, or in other words the transmitted bit value. The functions used for amplitude shifting generally should have a small low frequency content, a spectrum below the lowest frequency of the

filtered/masked signal, and should be mutually orthogonal. The particular choice of functions depends upon the specific application, and is specified in the stego key.

According to yet another alternative embodiment, a combination of different shifts in different domains can be executed simultaneously to generate a replica signal. For example, a time shift can be combined with a frequency shift, or an amplitude shift can be combined with a phase shift. Such a combination shift can further improve the hiding (security) property of the embedding system, and also improve detectability of the embedded signal by increasing the difference from the cover signal.

With respect to security, attacks would be expected that incorporate analysis designed to reveal the parameters of the stego key. If such parameters become known, then the embedded signal can be overwritten or obliterated by use of the same stego key. Use of a combination of shifts makes such analysis more difficult by enlarging the parameter space.

With respect to detectability, certain naturally occurring signals may have a content similar to a replica signal; for example, echo in an audio signal may produce a phase shifted signal, choral passages in a musical program may produce a frequency shifted signal, and tremolo may produce amplitude shifts, which may interfere with embedded signal detection. Use of a combination of shifts reduces the likelihood that a natural phenomenon will exactly match the parameters of the stego key, and interfere with signal detection.

The invention having been thus described, it will be apparent to those skilled in the art that the same may be varied in many ways without departing from the spirit and scope of the invention. Any and all such modifications as

would be apparent to those skilled in the art are intended to be covered by the following claims.

What is claimed is:

1. A method for embedding an auxiliary signal in an analog cover signal, comprising the steps of:

generating a replica signal from said cover signal;

modifying said replica signal as a function of said auxiliary signal; and

inserting the modified replica signal back into said analog cover signal.

2. A method according to claim 1, wherein the step of generating comprises the step of modifying at least a portion of said cover signal in a predetermined domain according to a stego key.

3. A method according to claim 2, wherein said predetermined domain is the frequency domain.

4. A method according to claim 2, wherein said predetermined domain is the time domain.

5. A method according to claim 2, wherein said predetermined domain is the spatial domain.

6. A method according to claim 2, wherein said replica signal is obtained by shifting the frequency of said at least one portion of said cover signal by a predefined amount specified by said stego key.

7. A method according to claim 2, wherein said replica signal is obtained by shifting the phase of said at least one portion of said cover signal by a predefined amount specified by said stego key.

8. A method according to claim 2, wherein said replica signal is obtained by shifting the amplitude of said at least one portion of said cover signal by a predefined amount specified by said stego key.

9. A method according to claim 2, wherein said replica signal is obtaining by shifting a predetermined combination of the frequency, phase, and/or amplitude of

said at least one portion of said cover signal by predefined amounts specified by said stego key.

10. A method according to claim 1, wherein the step of modifying comprises the step of multiplying said replica signal with said auxiliary signal.

11. A method for extracting an embedded auxiliary signal from an analog stego signal, comprising the steps of:

generating a replica signal from said stego signal;

modifying said stego signal as a function of said replica signal; and

extracting said information symbol by filtering said modified stego signal.

12. A method according to claim 11, wherein the step of generating comprises the step of modifying at least a portion of said stego signal in a predetermined domain according to a stego key.

13. A method according to claim 12, wherein said predetermined domain is the frequency domain.

14. A method according to claim 12, wherein said predetermined domain is the time domain.

15. A method according to claim 12, wherein said predetermined domain is the spatial domain.

16. A method according to claim 12, wherein said replica signal is obtained by shifting the frequency of said at least one portion of said stego signal by a predefined amount specified by said stego key.

17. A method according to claim 12, wherein said replica signal is obtained by shifting the phase of said at least one portion of said stego signal by a predefined amount specified by said stego key.

18. A method according to claim 12, wherein said replica signal is obtained by shifting the amplitude of said at least one portion of said stego signal by a predefined amount specified by said stego key.

19. A method according to claim 12, wherein said replica signal is obtained by shifting a predetermined combination of the frequency, phase and/or amplitude of said at least one portion of said stego signal by a predefined amount specified by said stego key.

20. A method according to claim 11, wherein the step of modifying comprises the step of multiplying said replica signal with said stego signal.

21. Apparatus for embedding and extracting auxiliary signals in an analog cover signal, comprising:

means for generating a replica signal from said cover signal;

means for modifying said replica signal as a function of said auxiliary signal;

means inserting the modified replica signal back into said analog cover signal to produce a stego signal;

means for receiving said stego signal;

means for generating a replica signal from said stego signal;

means for modifying said received stego signal as a function of said replica signal of said received stego signal; and

means for extracting said auxiliary signal by filtering said modified received stego signal.

22. Apparatus according to claim 21, wherein said means for generating a replica signal comprises means for modifying at least a portion of said cover signal in a predetermined domain according to a stego key.

23. Apparatus according to claim 22, wherein said predetermined domain is the frequency domain.

24. Apparatus according to claim 22, wherein said predetermined domain is the time domain.

25. Apparatus according to claim 22, wherein said predetermined domain is the spatial domain.

26. Apparatus according to claim 22, wherein said replica signal is obtained by shifting the frequency of said at least one portion of said cover signal by a predefined amount specified by said stego key.

27. Apparatus according to claim 22, wherein said replica signal is obtained by shifting the phase of said at least one portion of said cover signal by a predefined amount specified by said stego key.

28. Apparatus according to claim 22, wherein said replica signal is obtained by shifting the amplitude of said at least one portion of said cover signal by a predefined amount specified by said stego key.

29. Apparatus according to claim 22, wherein said replica signal is obtaining by shifting a predetermined combination of the frequency, phase, and/or amplitude of said at least one portion of said cover signal by predefined amounts specified by said stego key.

30. Apparatus according to claim 21, wherein said means for modifying said replica signal comprises means for multiplying said replica signal with said auxiliary signal.

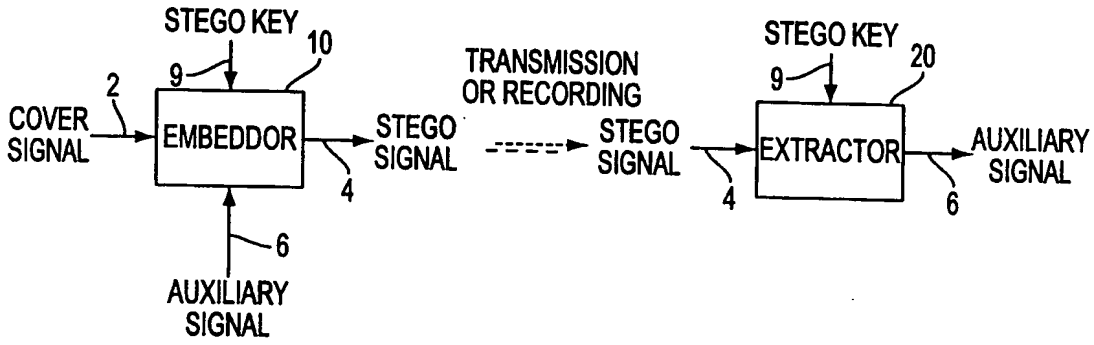

STEGO KEY
10
9
2
COVER SIGNAL
EMBEDDOR
STEGO SIGNAL
4
6
AUXILIARY SIGNAL
TRANSMISSION OR RECORDING
STEGO SIGNAL
STEGO KEY
20
9
EXTRACTOR
4
6
AUXILIARY SIGNAL

FIG. 1

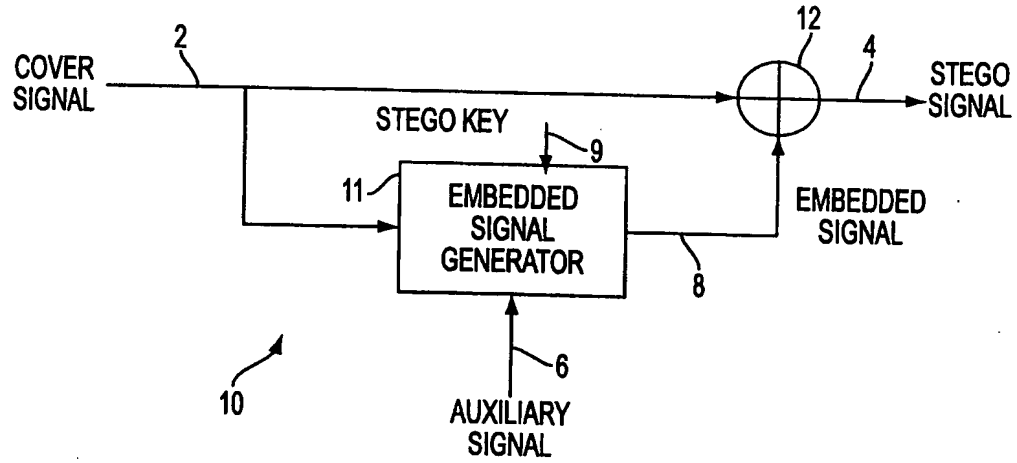

2
COVER SIGNAL
12
4
STEGO SIGNAL
STEGO KEY
9
11
EMBEDDED SIGNAL GENERATOR
8
EMBEDDED SIGNAL
10
6
AUXILIARY SIGNAL

FIG. 2

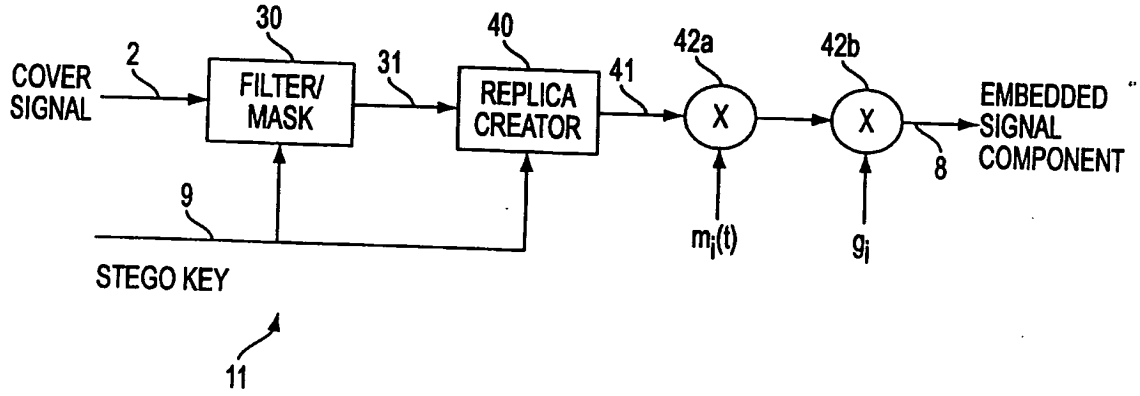

30
40
42a
42b
COVER SIGNAL
2
FILTER/ MASK
31
REPLICA CREATOR
41
X
X
EMBEDDED SIGNAL COMPONENT
8
9
STEGO KEY
$m_i(t)$
g_i
11

FIG. 3

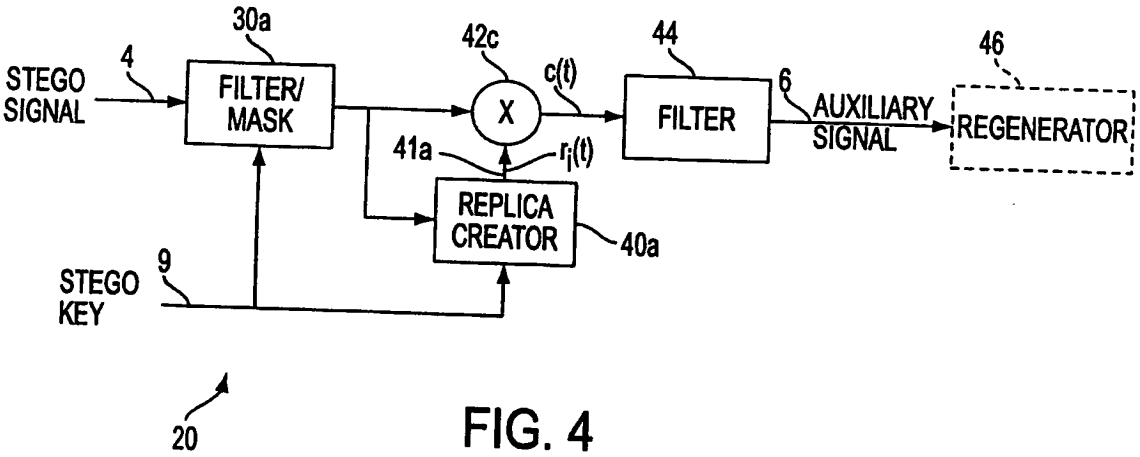

30a
42c
44
46
STEGO SIGNAL
4
FILTER/ MASK
X
c(t)
FILTER
6
AUXILIARY SIGNAL
REGENERATOR
41a
$r_i(t)$
REPLICA CREATOR
40a
STEGO KEY
9
20

FIG. 4

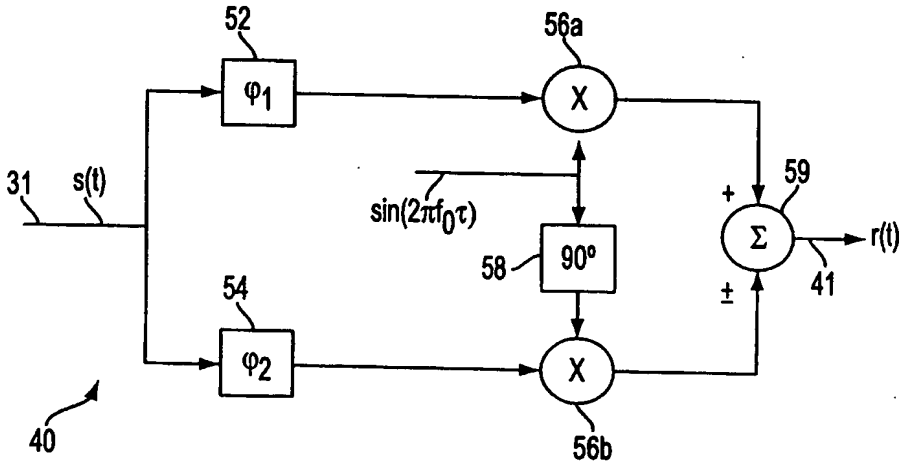


FIG. 5

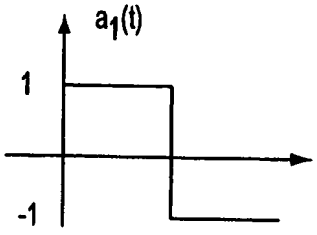


FIG. 6A

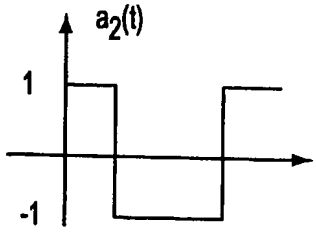


FIG. 6B

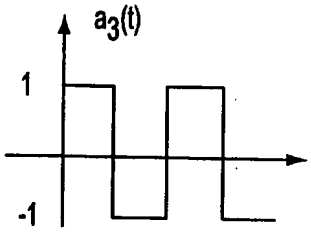


FIG. 6C

INTERNATIONAL SEARCH REPORT

Inte- ɔnal Application No
PCT/US 99/13482

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 H04H1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G11B H04H

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	WO 98 53565 A (ARIS TECHNOLOGIES INC) 26 November 1998 (1998-11-26) the whole document ---	1-30
X A	WO 97 09797 A (SOLANA TECHNOLOGY DEV CORP) 13 March 1997 (1997-03-13) abstract page 3, line 28 -page 10, line 28 page 18, line 2 - line 14 page 21, line 8 -page 22, line 22 claim 1; figure 1 --- -/--	1-4 6-14, 16-24, 26-30

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
29 October 1999	08/11/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Schiwy-Rausch, G

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Inte• ɔnal Application No
PCT/US 99/13482

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 33391 A (PLANKENBUEHLER ROLAND ;EBERLEIN ERNST (DE); PERTHOLD RAINER (DE);) 12 September 1997 (1997-09-12)	1
A	page 4, line 5 -page 5, line 24 page 10, line 19 -page 11, line 36 figure 1	2-5, 21-25
A	EP 0 372 601 A (PHILIPS NV) 13 June 1990 (1990-06-13) column 1, line 8 -column 3, line 12 column 7, line 3 -column 8, line 34 column 9, line 57 -column 12, line 11	1,11,21
A	WO 95 14289 A (PINECONE IMAGING CORP ;RHOADS GEOFFREY B (US)) 26 May 1995 (1995-05-26)	

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte· ɔnal Application No
PCT/US 99/13482

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9853565 A	26-11-1998	US 5940135 A	17-08-1999
WO 9709797 A	13-03-1997	US 5822360 A	13-10-1998
		AU 707270 B	08-07-1999
		AU 6899596 A	27-03-1997
		BR 9610469 A	30-03-1999
		CA 2231239 A	13-03-1997
		CN 1198275 A	04-11-1998
		EP 0852086 A	08-07-1998
		US 5937000 A	10-08-1999
WO 9733391 A	12-09-1997	DE 19640814 A	11-09-1997
		DE 19640825 A	11-09-1997
		AT 184140 T	15-09-1997
		DE 59700389 D	07-10-1999
		EP 0875107 A	04-11-1998
EP 0372601 A	13-06-1990	NL 8802769 A	01-06-1990
		NL 8901032 A	01-06-1990
		AT 118932 T	15-03-1995
		AU 626605 B	06-08-1992
		AU 4456889 A	31-05-1990
		DE 68921305 D	30-03-1995
		DE 68921305 T	07-09-1995
		ES 2071645 T	01-07-1995
		HK 61296 A	19-04-1996
		JP 2183468 A	18-07-1990
		KR 137473 B	15-06-1990
		US 5161210 A	03-11-1992
WO 9514289 A	26-05-1995	US 5768426 A	16-06-1998
		CA 2174413 A	26-05-1995
		EP 0737387 A	16-10-1996
		JP 9509795 T	30-09-1998
		US 5748763 A	05-05-1998
		US 5841978 A	24-11-1998
		US 5832119 A	03-11-1998
		US 5745604 A	28-04-1998
		US 5862260 A	19-01-1999
		US 5841886 A	24-11-1998
		US 5850481 A	15-12-1998